ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Online Examination System Based On Student Authentication Using LTP& OTP

Misal Vijaya Balu, Nare Payal Rajendra, Udare Sanjana Sanjay.

B.E. Student, Department of Computer Engineering, V.A.C.O.E. Ahmednagar, Maharashtra, India

ABSTRACT: Online examination systems are in a huge demand. Even though there are a wide range of online examination systems they have not successfully replaced the tradition examination system as tradition examination system require descriptive answers with diagrams. This system which gives permission to an organization, company or institute to arrange, conduct and manage examinations via an online environment. This can be done through the Internet, Intranet and/or Local Area Network environments. In this implementation, we proposed a system that facilitates online examination system to improve online examination by utilizing various technologies such as internet-firewall, cryptography, network protocol and object oriented paradigms. An examination system is designed and developed based on web. This paper describes the principle of the system, presents the main functions of the system, analyses the algorithm of auto- generating test paper, and discusses the security of the system.

KEYWORDS: Online Exam, Randomization, Security, Algorithm, Examination Command Centre, Network security.

I. INTRODUCTION

At present, the traditional test method is mainly based on paper. The shortcoming of this method is overload of work, delay of statistics and evaluation, error-prone, etc. With the popularity of computer and the development of the network, we need a new test platform to solve these problems. Combined with the actual demand, we design and develop a set of simple, convenient, safety good online examination system based on Web. Online Examinations, sometimes referred as e-examinations, are the examinations conducted through the internet or in an intranet (if within the Organization). Online examination system is proposed for universities, colleges and schools, even Banking, Government for recruitment purposes. Today many organizations are conducting online examinations worldwide successfully and produce the results in online. The system is designed to conduct exam or test by online and the results will automatically uploaded in the student’s mail. Exam System is very useful for Educational Institute to prepare an exam, safe the time that will take to check the paper and prepare mark sheets. Online Examination System (OES) is a Multiple Choice Questions (MCQ) based on examination system that provides an easy to use environment for both Test Conductors and Students appearing for Examination. This system is secure information is provided to user. The system should be designed in as a secured system applying safety measures. Special exception handling mechanism should be in place to avoid system errors. In case of scenarios where data integrity could be compromised, measures should be taken to ensure that all changes are made before system is shut down. The system is consisting of a web based server with a database facility. Database it contains user information and authentication for the examination. This server is configured with proper security measures. Candidates can connect through the internet with a web browser (e.g. Internet Explorer, Mozilla Firefox etc) or Intranet or using a small application in candidate system to connect the server and take the examination.

II. RELATED WORK / SURVEY

A. Online Examination System for University Level Descriptive Examinations[4.]

Online examination systems are in a huge demand. In the current era there are various system were designed based on the online examination system and these system have not successfully replaced the traditional examination system as tradition examination system require descriptive answers with diagrams. Especially for University level examinations like Engineering and Medical Science students knowledge is judged based on the concepts she/he has gained from the course and the applications of such knowledge is evaluated in the examinations and to manage and support such type of

DOI: 10.15680/IJIRCCE.2017. 0505137

examinations we require a system that will allow candidates to answer the questions in details and in a correct way with appropriate diagrams to support their explanations.

B.Challenges of Online Exam, Performances and problems for Online University Exam[3.]

In this system that provides security to improve on-line examination by utilizing technologies such as biometric authentication, internet-firewall, cryptography, network protocol and object oriented paradigms. Furthermore, we propose a framework for conducting online exams through insecure internet backbone. The system will facilitates a secure communication based cryptography and group communications. In the research paper, we describe and explain deeply, the performance of students online course exam with respect to security and challenges faced by online course exams within the university. We conclude that by improving the security system using biometrics face recognition that can be incorporated into the proposed system to fulfill the challenge of online exam.

C.Design and Implementation of Secure Computer Based Examination System Based On B/S Structure.

Online Examination System is efficient, fast and reduces the large amount of material resources. In this paper, proposed secure computer based examination system base on B/S structure to address these aforementioned drawback. The system is designed to facilitate the exam process, manage surrounding the conduct of any type of examination (Academic institution, company, School), support Multilanguage question, random question display at a time, solution to the issue of security and cheating for online exams The new system was design and implement using HTML, JAVASCRIPT, JQUERY, AJAX, JSP and MYSQL database which may be deployed on either on internet or Intranet. The analysis of this system as well as testing of this system is done in the real environment.

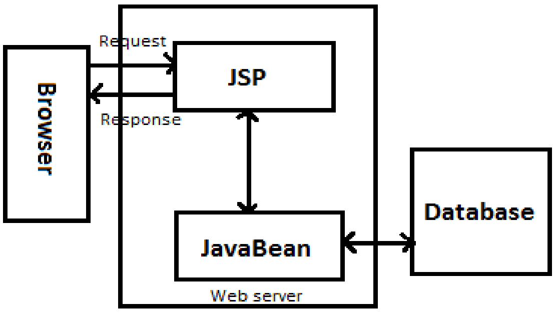


Figure 1: B/S System Architecture

D.The Design and Implementation of On-Line Examination Using Firewall security[1]

The proposed online examination system is a software solution, which allows a company or institute to arrange, conduct and manage examinations via an online environment. This can be done through the Intranet, Internet or Local Area Network (LAN) environments. In this paper propose a system that provides security to improve on-line Examination by utilizing DMZ Concept in firewall technology. This paper concludes that by improving the security system using a firewall system that can be incorporated into the proposed system to fulfil the challenge of online examination system. We proposed a system using firewall technology to monitor candidates and control network packets of all machines incorporating the username and password for authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

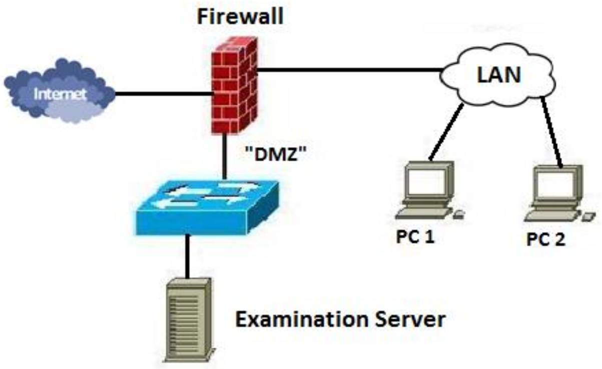


Figure 2: Firewall with network security

III. PROPOSED SYSTEM

The proposed system is as described below:

- The proposed system facilitates us a strong and secure online examination system. The proposed system consists mainly three modules: user management, test management, and score management.
- Firstly, in registration phase users completes their registration for online exam. In between registration phase a long time password (LTP) will receive in user's email id.
- User management is responsible for handling the information of administrators and students. While test management includes the functions for student or administrators to select randomly questions from database to generate test papers.
- Score management is in charge of the automatic scoring of test papers and giving the corresponding feedbacks to students.
- When students appear for online exam then system generates one time password (OTP) and the combination of LTP and OPT with some mathematical operations which will shown on the screen of computers after that students will able to do his/her question paper.
- The questions of test paper will generate randomly in every computer.
- Only admin will have authority to see every student's result and according to the criteria the link of score card or result will be forward to student's email.

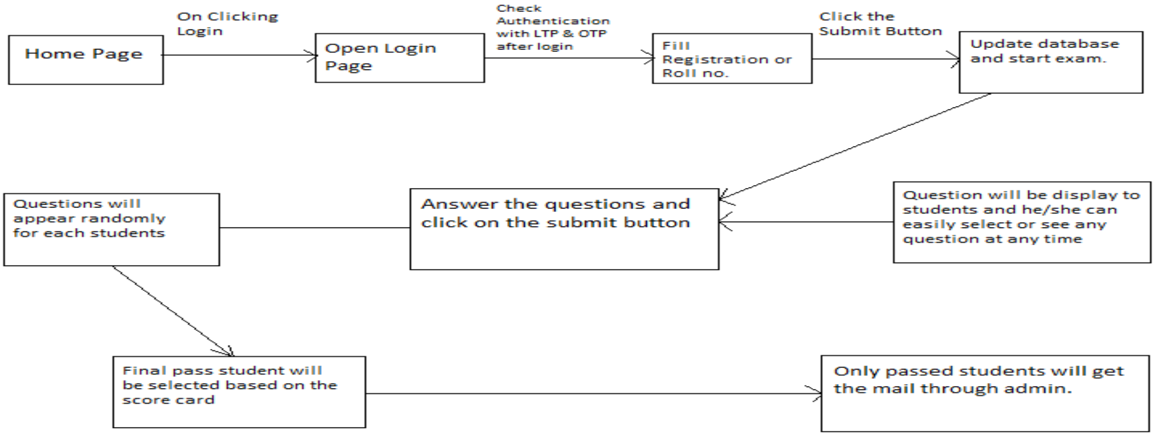

Home Page
On Clicking Login
Open Login Page
Check Authentication with LTP & OTP after login
Fill Registration or Roll no.
Click the Submit Button
Update database and start exam.
Question will be display to students and he/she can easily select or see any question at any time
Answer the questions and click on the submit button
Questions will appear randomly for each students
Final pass student will be selected based on the score card
Only passed students will get the mail through admin.

Figure:3 Proposed System Architecture

IV. ALGORITHM

AES Algorithm

AES is a new cryptographic algorithm which can be used to protect electronic data. AES is a block cipher of symmetric-key which are use the keys of 128, 192, and 256 bits, and encrypts as well as decrypts contents in blocks of 128 bits. AES use a keys pair, the same key use by the symmetric-key ciphers to encryption and decryption of data. The same number of bits have the data which encrypted which obtained by block ciphers that the input data had. A loop structure use by Iterative ciphers that permutations as well as substitutions of the input data performs repeatedly.

The AES algorithm is depends on permutations and substitutions. Permutations means that rearrangements of data, and substitutions is the replacement of the data i.e. replace one unit of data with another. Using several different techniques, AES performs permutations and substitutions.

The AES cipher key size represents the number of repetitions of transformation rounds which performs conversion the input, which is known as the plaintext, into the final output, which is known as the ciphertext. Following there are shows the number of cycles of repetition:

•For 128-bit keys 10 cycles of repetition

•For 192-bit keys 12 cycles of repetition.

•For 256-bit keys 14 cycles of repetition.

Several processing steps are consist by each round, each containing four similar but which are different stages. In those, one that based on the key encryption itself. To transform cipher text back into the original plaintext, a set of reverse rounds are applied using the same encryption key.

Description

1.Key Expansions

For each round AES needs a different 128-bit block of round key also one more.

2.Initial Round

AddRoundKey- with a block of the round key, each byte of the state is combined using bitwise xor.

3.Rounds

•Sub Bytes—in this step each byte is replaced with another byte.

•Shift Rows— for a certain number of steps, the state's last three rows are moved cyclically.

Mix Columns— on the columns of the state a mixing operation operates, in each column combining the four bytes.

- AddRoundKey

4. Final Round (no Mix Columns)

- Sub Bytes
- Shift Rows
- AddRoundKey.

The Sub Bytes step

In the Sub Bytes step, using an 8-bit substitution box, with a Sub Byte each byte in the state matrix is replaced. In the cipher, the nonlinearity provided by this operation. From the multiplicative inverse over GF (28) the S-box used is derived, known to have good non-linearity properties. By combining the inverse function The S-box is constructed with an inverse transformation to avoid attacks which is depends on properties of simple algebraic. The S-box and also any opposite fixed points is also chosen for to avoid of any fixed points, for performing the decryption, Sub Bytes step is used inversely, for that, before obtaining the inverse of multiplication, first taking the affine transformation.

The Shift Rows step

On the rows of the state, the Shift Rows step operates; it shifts the bytes in each row cyclically by a certain offset. The first row is left unchanged, for AES. Each byte is shifted one to the left of the second row. Similarly, by the offsets of two and three the third and fourth rows are shifted. The shifting pattern is the same, for blocks of sizes 128 bits and 192 bits, by n-1 bytes, circularly row n is shifted left. In this way, from each column of the input stat, the output state's each column of the Shift Rows step is composed of bytes e. The first row is unchanged, for a 256-bit block and 1 byte, 3 bytes and 4 bytes needs for the shifting for the second, third and fourth row respectively. When used with a 256-bit block, as AES doesn't use 256-bit blocks, for the Rijndael cipher this change applies. The case like to avoid the columns being linearly independent, is the importance of this step. The degeneration of AES into four individual ciphers of block.

The Mix Columns step

With a fixed polynomial in the Mix Columns step each column of the state is multiplied. In the Mix Columns step, combined Using an invertible linear transformation, every column of the state are have four bytes. As input needs for The Mix Columns function is four bytes and there also four bytes of output, where all four output bytes affects by each input byte. Mix Columns provides diffusion in the cipher, together with Shift Rows.

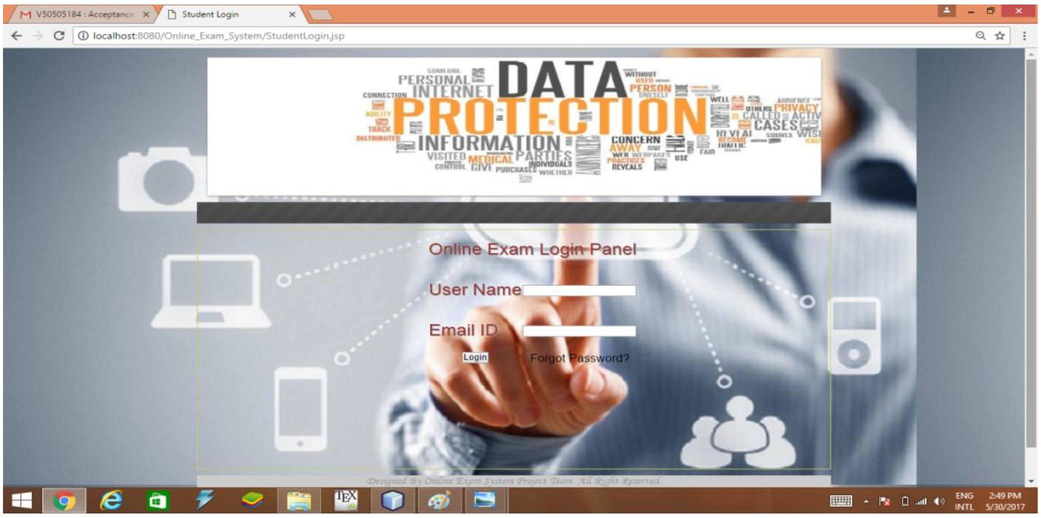
The AddRoundKey step

In this step, with the state there are combination of the sub key is combined. From the main key a sub key is derived, for every round with the help of Rijndael's key schedule; there are same size for every sub key as the state. Using bitwise XOR, by combining every byte of the state with the corresponding byte of the sub key, the sub key is added.

V. GOALS AND OBJECTIVE

The objectives of the "Online Examination system" are as follows:
1. To replace paper base examination system into Online base examination System.
2. For all students and professionals, it is very important to have some basic understanding about the online examination system.
3. Online examination will reduce the hectic job of assessing the answers given by the candidates manually.
4. Random generation of test question timed examed.
5. To reduces the large amount of material resource.
6. The result will be shown immediately to the participating students.
7. To provide more security as compare to offline examination system in terms of paper leakage.

VI. RESULT

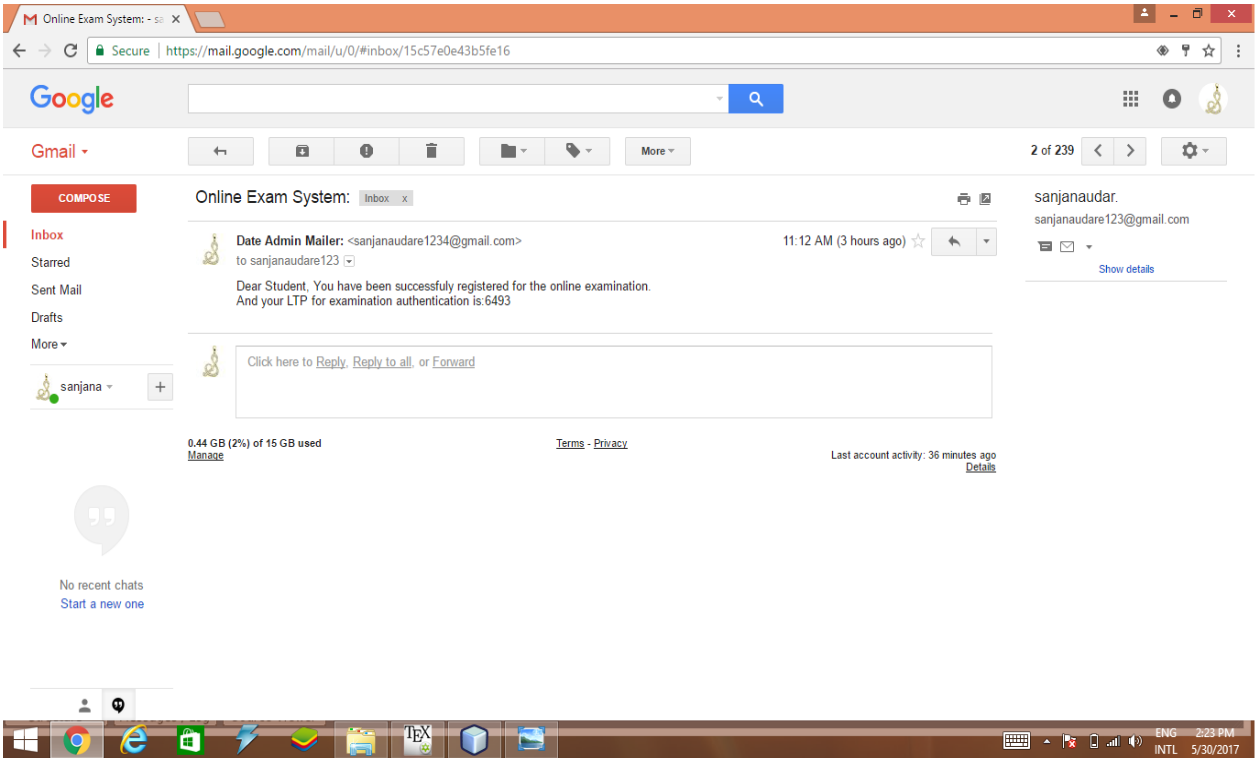

V50505184 : Acceptance
Student Login
localhost:8080/Online_Exam_System/StudentLogin.jsp

Online Exam Login Panel
User Name
Email ID
Login
Forgot Password?

Designed By Online Exam System Project Team. All Right Reserved.

Figure4. Student Login Form

DOI: 10.15680/IJIRCCE.2017. 0505137



Online Exam System: Inbox

Date Admin Mailer: <sanjanaudare1234@gmail.com> 11:12 AM (3 hours ago)
to sanjanaudare123

Dear Student, You have been successfuly registered for the online examination.
And your LTP for examination authentication is:6493

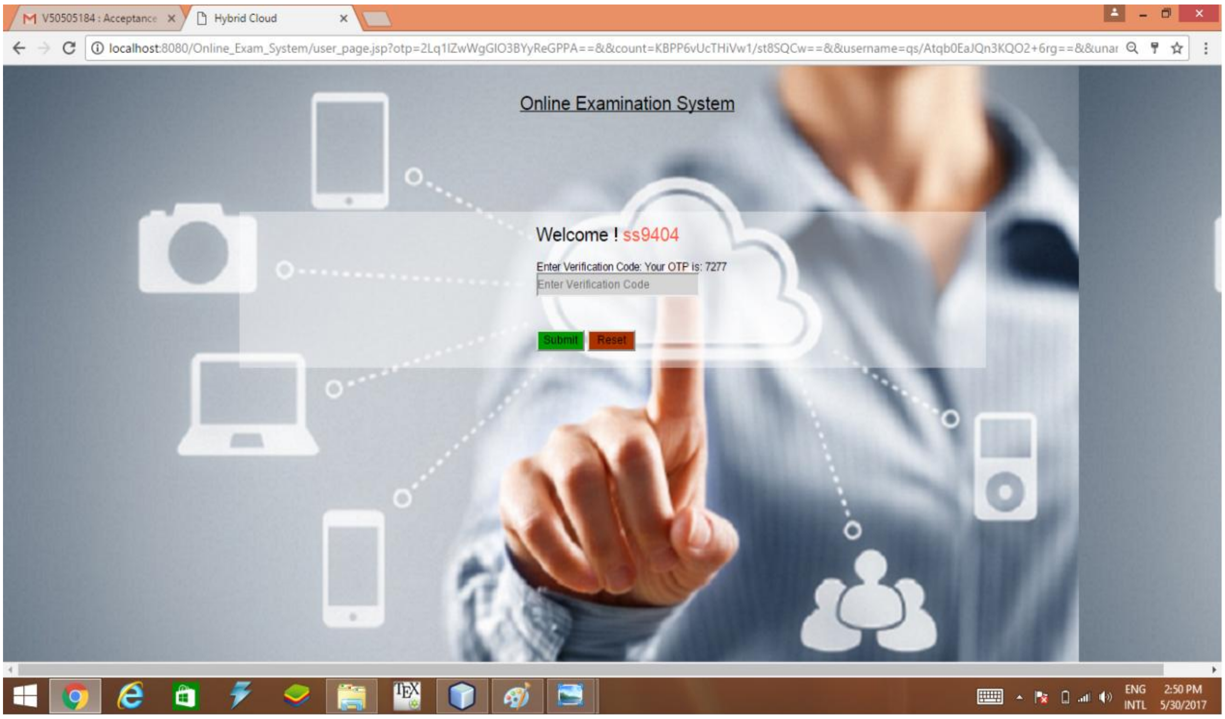
Click here to Reply, Reply to all, or Forward

0.44 GB (2%) of 15 GB used
Manage

Terms - Privacy

Last account activity: 36 minutes ago
Details

Figure5. Provide LTP Through Mail


V50505184 : Acceptance
Hybrid Cloud
localhost:8080/Online_Exam_System/user_page.jsp?otp=2Lq1lZwWgGIO3BYyReGPPA==&&count=KBPP6vUcTHiVw1/st8SQCw==&&username=qs/Atqb0EaJQn3KQO2+6rg==&&unar

Online Examination System

Welcome ! ss9404

Enter Verification Code: Your OTP is: 7277

Enter Verification Code

Submit Reset

Figure6. Provide OTP at time of exam

DOI: 10.15680/IJIRCCE.2017. 0505137

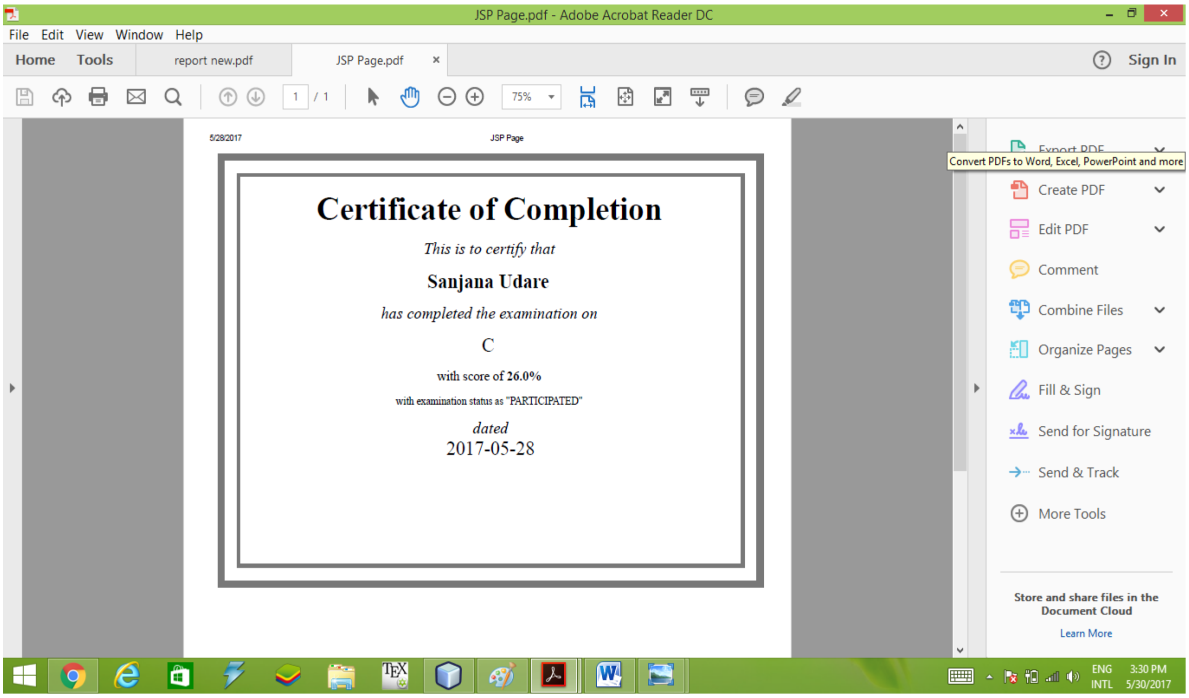
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017


JSP Page.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools report new.pdf JSP Page.pdf
Sign In
75%
Export PDF
Convert PDFs to Word, Excel, PowerPoint and more
Create PDF
Edit PDF
Comment
Combine Files
Organize Pages
Fill & Sign
Send for Signature
Send & Track
More Tools
Store and share files in the Document Cloud
Learn More
ENG INTL 3:30 PM 5/30/2017

5/28/2017 JSP Page

Certificate of Completion

This is to certify that

Sanjana Udare

has completed the examination on

C

with score of **26.0%**

with examination status as "PARTICIPATED"

dated

2017-05-28

Figure7. Provide Certificate After Examination

VII. Conclusion and Future Work

This system will reduce a lot of physical exercise done by the college and universities in conducting and maintaining a strong room for storing the answer scripts of the candidates. The college is responsible for submitting the answer scripts to the university at the end of the exam. This task is no more needed as the digital papers are submitted into the centralized server directly. In this paper mainly focused on to Conduct an Online Examination System in more secure way. In this paper, we have proposed and discussed OTP and LTP based online examination system. We design and develop the online examination system. This system overcomes the defects of the traditional detection method based on paper, and improves the efficiency as well as security of online examination system.

References

[1] V.Selvi1, R.Sankar and R.Umarani, "The Design and Implementation of On-Line Examination Using Firewall security" in IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. V (Nov-Dec. 2014), PP 20-24 www.iosrjournals.org

[2] Sanjay Kr. Singh and Arvind Kr. Tiwari, "Design and Implementation of Secure Computer Based Examination System Based On B/S Structure", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016) pp 312-318 Research India Publications.

[3] Md. A. Sarrayrih1 and Md. Ilyas, "Challenges of Online Exam, Performances and problems for Online University Exam", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 ISSN (Online): 1694-0814.

[4] VijaylaxmiPatil, M. S. Emmi and P.V.Gajanan, "Online Examination System for University Level Descriptive Examinations", International Journal on Recent and Innovation Trends in Computing and Communication Volume:2 Issue:9, ISSN: 2321-8169, 2649-2651.

[5] HongmeiNie, "Design and Development of the Online Examination System Based on B/S Structure", 2nd International Conference on Teaching and Computational Science (ICTCS 2014).

[6] Umed H. Suthar1, Prof. Abdul Rais 2, Ashish Upadhyay3, Prabhakar Upadhya4 "Online Examination Management System Using Genetic Algorithm" International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 5, Sep-Oct 2015.

[7] DeepankarVishwas Kotwal1, ShubhamRajendra Bhadke2, Aishwarya Sanjay Gunjal3, PuspenduBiswas4 "ONLINE EXAMINATION SYSTEM" International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 01 | Jan-2016.

[8] Vishnu Patidar1, Vishal Kadam2 "Analysis Process ofDesign and Development of Online Examination System"International Journal ofInnovative Research in ComputerandCommunication Engineering Vol. 4, Issue 2, February 2016.